IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Massimiliano Antonio Poletto et al.	Art Unit	: 2135
Serial No.	: 09/931,344	Examiner	: Ha, L.
Filed	: August 16, 2001	Conf. No.	: 2635
Title	: DEVICE TO PROTECT VICTIM SITES DURING DENIAL OF SERVICE ATTACKS		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF ON BEHALF OF MASSIMILIANO ANTONIO POLETTO ET AL

Please charge the Appeal Brief fee of **$250** to Deposit Account No. 06-1050. If an additional fee is due, please apply that fee and any other charges or credits to Deposit Account No. 06-1050.

(i.) Real Party In Interest

The real party in interest in the above application is Mazu Networks, Inc.

(ii.) Related Appeals and Interferences

The appellant is not aware of any appeals or interferences related to the above-identified patent application.

(iii.) Status of Claims

This is an appeal from the decision of the Primary Examiner in an Office Action dated April 18, 2006, rejecting claims 1-39, all of the claims in the application. Claims 1-39 are the subject of this appeal.

(iv.) Status of Amendments

Appellant filed a Reply to the Final Office Action amending claims 1 and 16 to correct the informalities pointed out by the examiner and incorporate a portion of the preamble into the body of those claims.

In an advisory action dated July 20, 2006, the examiner did not enter the amendment indicating that amendments to claims 1 and 16 required further consideration and or seach. Accordingly, the claims on appeal are those that existed prior to the final action. Appellant filed a Notice of Appeal on **October 19, 2006**.

(v.) Summary of Claimed Subject Matter

Claim 1

One aspect of Appellant's invention is set out in claim 1 as a gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device comprises a computing device. "The arrangement 10 to protect the victim includes a control center 24 that communicates with and controls gateways 26 and data collectors 28 disposed in the network 14. The arrangement protects against DoS attacks via intelligent

traffic analysis and filtering that is distributed throughout the network." [Appellant's specification Page 5, lines 17-22].

Inventive features of claim 1 include a monitoring process that monitors network traffic through the gateway. "The gateway 26 includes a monitoring process 32 (FIG. 6B) that monitors traffic that passes through the gateway ... ." [Appellant's specification Page 7, lines 9-10].

Inventive features of claim 1 also include a communication process that communicates statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center. "... as well as a communication process 33 that can communicate statistics collected in the gateway 26 with the data center 24." [Appellant's specification Page 7, lines 10-13].

Inventive features of claim 1 also include a filtering process to insert filters on network devices to filter out packets that the gateway deems to be part of an attack. "In addition, the gateway 26 can include processes 35 to allow an administrator to insert filters to filter out, i.e., discard packets that the device deems to be part of an attack, as determined by heuristics described below." [Appellant's specification Page 7, lines 17-20].

Claim 16

Another aspect of Appellant's invention is set out in claim 16 as a method of protecting a victim site during a denial of service attack. Appellant's originally filed claims and summary discuss a method.

Inventive features of claim 16 include disposing a gateway device between the victim site and a network. "Referring to FIG. 2, details of an exemplary deployment of a gateway is shown. Other deployments are possible and the details of such deployments would depend on characteristics of the site, network, cost and other considerations. The gateway 26 is a program executing on a device, e.g., a computer 27 that is disposed at the edge of the data center 20 behind an edge router at the edge of the Internet 14." [Appellant's specification Page 6, line 27 to Page 7, line 2].

Inventive features of claim 16 also include monitoring network traffic through the gateway and measuring heuristics of the network traffic to provide statistics network traffic. This feature finds support as the analogous feature of claim 1.

Inventive features of claim 16 also include communicating the statistics collected in the gateway to a control center. This feature finds support as the analogous feature of claim 1.

Inventive features of claim 16 also include filtering out packets that the gateway or control center deems to be part of an attack. This feature finds support as the analogous feature of claim 1.

Claim 29

Another aspect of Appellant's invention is set out in claim 29 as a computer program product residing on a computer readable medium for protecting a victim site during a denial of service attack, comprises instructions for causing a computer device coupled at an entry to the site to. "The gateway 26 and data collector 26 are typically software programs that are executed on devices such as computers, routers, or switches." [Appellant's specification Page 9, lines 6-9].

Inventive features of claim 29 include instructions to monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic. This feature finds support as the analogous feature of claim 1.

Inventive features of claim 16 also include instructions to communicate statistics collected in the computer device to a control center. This feature finds support as the analogous feature of claim 1.

Inventive features of claim 16 also include instructions to filter out packets that the device or control center deems to be part of an attack. This feature finds support as the analogous feature of claim 1.

(vi.) Ground of Rejection to be Reviewed on Appeal

Claims 1-39 stand rejected under 35 U.S.C. 102(e) as being anticipated by Yavatkar, et al. (US 6,735,702).

(vii.) Argument

Anticipation

"It is well settled that anticipation under 35 U.S.C. §102 requires the presence in a single reference of all of the elements of a claimed invention." *Ex parte Chopra*, 229 U.S.P.Q. 230, 231 (BPA&I 1985) and cases cited.

"Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983).

"This court has repeatedly stated that the defense of lack of novelty (i.e., 'anticipation') can only be established by a single prior art reference which discloses each and every element of the claimed invention." *Structural Rubber Prod. Co. v. Park Rubber Co.*, 223 U.S.P.Q. 1264, 1270 (Fed. Cir. 1984), citing five prior Federal Circuit decisions since 1983 including *Connell*.

In a later analogous case the Court of Appeals for the Federal Circuit again applied this rule in reversing a denial of a motion for judgment n.o.v. after a jury finding that claims were anticipated. *Jamesbury Corp. v. Litton Industrial Prod., Inc.*, 225 U.S.P.Q. 253 (Fed. Cir. 1985).

After quoting from *Connell*, "Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim," 225 U.S.P.Q. at 256, the court observed that the patentee accomplished a constant tight contact in a ball valve by a lip on the seal or ring which interferes with the placement of the ball. The lip protruded into the area where the ball will be placed and was thus deflected after the ball was assembled into the valve. Because of this constant pressure, the patented valve was described as providing a particularly good seal when regulating a low pressure stream. The court quoted with approval from a 1967 Court of Claims decision adopting the opinion of then Commissioner and later Judge Donald E. Lane:

> [T]he term "engaging the ball" recited in claims 7 and 8 means that the lip contacts the ball with sufficient force to provide a fluid tight seal **** The Saunders flange or lip only sealingly engages the ball 1 on the upstream side when the fluid pressure forces the lip against the ball and never

> scalingly engages the ball on the downstream side because there is no fluid pressure there to force the lip against the ball. The Saunders sealing ring provides a compression type of seal which depends upon the ball pressing into the material of the ring. *** The seal of Saunders depends primarily on the contact between the ball and the body of the sealing ring, and the flange or lip sealingly contacts the ball on the upstream side when the fluid pressure increases. 225 U.S.P.Q. at 258.

Relying on *Jamesbury*, the ITC said, "Anticipation requires looking at a reference, and comparing the disclosure of the reference with the claims of the patent in suit. A claimed device is anticipated if a single prior art reference discloses all the elements of the claimed invention as arranged in the claim." *In re Certain Floppy Disk Drives and Components Thereof*, 227 U.S.P.Q. 982, 985 (U.S. ITC 1985).

Claims 1-39 are not anticipated by Yavatkar.

Claims 1, 3, 4, 14, 15, 16, 18, 19 and 28

For the purposes of this appeal only, claims 1, 3, 4, 14, 15, 16, 18, 19 and 28 stand or fall together. Claim 1 is representative of this group of claims.

Claim 1 is directed to a gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, with the gateway including a computing device. Yavatkar neither describes nor suggests a computing device that includes… a communication process that communicates statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center and a filtering process to insert filters on network devices to filter out packets that the gateway deems to be part of an attack."

The examiner contends that:

> **As per claim 1:**
> **Yavatkar discloses gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device comprises: a computing device comprising:**
> **a monitoring process that monitors network traffic through the gateway; [col. 1, lines and col.7, lines 43-48]**

> a communication process that communicate statistics collected [col.2, lines 4-5 and 53-60 and col.3, lines 28-45, statistics from the monitoring process is inherently gathered data of similarities or differences used for analysis purposes to determine the attacks and kind of traffic on the gateway.] in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center; [col.3, lines 25-29 and col. 11, lines 51-55] and
>
> a filtering process to insert filters on network devices [col.3, lines 46-53 and col. 13, lines 56-62] to filter out packets that the gateway deems to be part of an attack. [col.20, lines 20-21] (Emphasis in original omitted) [1]

Yavatkar fails to describe or suggest a communication process that communicates statistics collected in the gateway by the monitoring process to a control center and that receives queries or instructions from the control center. The examiner contends that Yavatkar discloses this feature at Col 2, lines 4-5. Rather, Appellant contends that Yavatkar discloses: "A sniffer is a device which may record network statistics at a node."[2] Similarly, Yavatkar discloses: "Worksheets 234-38 may perform tasks such as monitoring port statistics, CPU utilization, or reachability to other nodes."[3]

Neither of these teachings describes or suggests the claimed feature of: "a communication process that communicates statistics collected in the gateway by the monitoring process to a control center and that receives queries or instructions from the control center."

The examiner also argues that: "statistics from the monitoring process is (sic) inherently gathered data of similarities or differences used for analysis purposes to determine the attacks and kind of traffic on the gateway."[4] Appellant again disagrees. With respect to the "sniffer" device Yavatkar teaches that the sniffer is a prior art technique that is slow and inaccurate. According to Yavatkar:

> For example, to determine the node which is the source of attack traffic (or the gateway allowing such traffic into a network, which in such a case may be considered a source) and the path or paths taken by such traffic, a human operator may access each link at a node receiving such traffic and analyze the incoming traffic using a sniffer. A sniffer is a device which may record network statistics at a node. The operator may identify which of the physical links attached to the node is receiving a certain type or amount of traffic and then move to the node on the other end of the identified link. The path or paths of traffic from the source of the traffic may be found by traversing the network from node to node, using the sniffer at each node in a path, until the source is reached.

[1] Final Office Action pages 2-3
[2] Yavatkar at Col 2, lines 4-5
[3] Id at Col. 10, lines 15-16,
[4] Final Action page 3.

While it is arguable whether the disclosed sniffer "records network statistics at a node" meets the claimed feature of "...statistics collected in the gateway from the monitoring process ...," it is quite clear that Yavatkar clearly discloses that it is the operator that may identify which physical link attached to the node received a certain type or amount of traffic and then move to the node on the other end of the link. However, this does not teach the features of a monitoring process that monitors network traffic through the gateway and a communication process that communicates statistics collected in the gateway by the monitoring process to a control center and that receives queries or instructions from the control center.

Indeed, Yavatkar also does not teach the claimed communication process by the disclosed "Worksheets 234-38." Yavatkar discloses worksheets as part of an agent 110:

> **In an exemplary embodiment agent 110 includes code segment 220, which is comprised of Java[4] methods which are members of agent 110 and which provide functionality to agent 110; and state 230. Code segment 220 includes work object 222 providing functionality to agent 110. State 230 includes worksheets 234, 236 and 238; work object 222 may use worksheets 234-38 to provide functionality to agent 110. Worksheets 234-38 are members of agent 110 which may be Java[4] or non-Java[4] language code segments.[5]**

Yavatkar does not disclose any feature of the control center with these teachings. Moreover, because Yavatkar discloses a "sniffer" as an element of the prior art, which he strongly criticizes, and discloses "Worksheets" as part of the state of the disclosed agents 110, it cannot not follow that the examiner has made out a case of prima facie anticipation, since there is no disclosure in Yavatkar that uses the combined functionality of the sniffer and the worksheets. Therefore, assuming *arguendo* that somehow these two passages did teach the claimed feature, the examiner still has not made out a prima facie anticipation case, since these features are disclosed as disconnected and incompatible and indeed one feature is criticized by Yavatkar. Therefore, Yavatkar could not meet the test to establish anticipation, as set forth by the Federal Circuit: "Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983).

---

[5] Yavatkar, Col. 10, lines 5-14

Yavatkar also discloses agents, "mobile software modules" to collect data on the state of a network during a network attack. However, Yavatkar also discloses that an agent manages devices via services provided on a proxy device to monitor or control managed devices.[6] Yavatkar says nothing that could suggest a communication process that communicate statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center. Yavatkar's disclosed agents do not communicate statistics collected in the gateway or receives queries from a control center. Neither the agent nor the sniffer receives queries from a communication process running on a gateway.

Claim 1 also requires a filtering process to insert filters on network devices to filter out packets that the gateway or the control center deems to be part of an attack.

Yavatkar however teaches to either shut down the gateway or to insert filters with the conventional sniffer.[7] However, in Yavatkar, that decision is performed by an administrator using a sniffer that determines a physical link or certain modules under direction of a central console[8] not as in claim 1 where a computing device includes a filtering process the filter removes packets that the gateway deems to be part of the attack. Yavatkar also discloses that with such information a network administrator moves from node to node, tracing the path of the hostile messages from the victim to the source or to the gateway allowing such traffic to enter the network. Yavatkar acknowledges that such a method of determining the source of messages is slow. Yavatkar proposes to address this by use of watchdog and bloodhound agents.[9] Therefore, Yavatkar fails to teach the "gateway device comprises… a filtering process to insert filters on network devices to filter out packets that the gateway deems to be part of an attack."

Appellant contends therefore that Yavatkar must fail as an anticipating reference because Yavatkar fails to describe that the gateway includes a computing device, disposed between a data center and a network with the computing device executing a monitoring process … a communication process and a filtering process, as claimed. The examiner's anticipation rejection is a concoction of unrelated elements from Yavatkar that existed in three separate

[6] See Yavatkar col. 11, lines 46-55.
[7] Yavatkar Col. 13, lines 54-58
[8] Yavatkar Col. 13, line 63 to Col. 14, line 2.
[9] Yavatkar discussion starting at Col. 14, line 18.

unrelated mechanisms. However, this does not constitute an anticipation reference since although assuming *arguendo* that these mechanisms have some individual relevance to the claimed features, they are not described as existing together. Thus, Yavatkar cannot describe the claimed gateway, since there is no device or structure in Yavatkar that possesses all of the features of the claimed gateway. Thus, assuming that the examiner is correct that elements from claim 1 are found in the reference, it is patently clear that those elements are not arranged in the reference in a manner as they are arranged in the claim.

For example, the monitoring process the examiner finds[10] in col. 1, lines and col.7, lines 43-48. However, this is a discussion of the prior art that Yavatkar criticizes and is not described as being included in any device described by Yavatkar, whereas, col. 7, lines 43-48 pertain to discussion of a gateway. Specifically Yavatkar discloses that: "Node 48 is a gateway, providing network 4 access to other networks, such as the Internet, and acting as a firewall. Link 84 transmits data between node 48 and other networks."[11] However, that gateway is not described as performing any of the claimed functions.

For the communication process the examiner relies[12] on col.2, lines 4-5, which is a discussion of a prior art "sniffer." and 53-60, which is a discussion of his inventive concept, which does not indicate any use for the "sniffer." Similarly col.3, lines 28-45 is a discussion of two different mobile agents that collect data on the state of the network.

For the filtering process to insert filters on network devices the examiner relies[13] on col.3, lines 46-53 discussion of watchdog and bloodhound agents and col. 13, lines 56-62 discussion of a gateway that can be shut down or have filters installed. While Yavatkar does mention a prior art method, namely:

> **However, using current methods to identify the gateway which is, in effect, the source of attack traffic to the network can be difficult and time consuming. A network administrator using a sniffer may determine which physical link (of multiple links) on a device receiving attack traffic is the source of such traffic. Certain modules resident on nodes may perform similar functions under the direction of a central console. With such information a network administrator may**

[10] Final Action page 3
[11] Yavatkar col. 7, lines 43-48
[12] Final Action page 4
[13] Id.

> **move from node to node, tracing the path of the hostile messages from the victim to the source, or to the gateway allowing such traffic to enter the network. Such a method of determining the source of messages is slow.[14]**

Yavatkar teaches away from any combination of a "sniffer" device arguing that it is a conventional method and is slow.

The teachings that the examiner relies on in Yavatkar are to elements that area on different devices. The devices perform somewhat similar, but not identical functions, as the claimed gateway. However, the claimed gateway is a computing device that performs all of the functions recited. Yavatkar does not show any device that performs all of the recited functions and indeed given the rejection as concocted by the examiner, it would be inconsistent with Yavatkar to have a single device perform all of the claimed functions.

Therefore, Yavatkar is not an anticipating reference since Yavatkar fails to describe all of the claimed features and fails to describe a device that possesses all of the clamed features arranged as in the claim.

The examiner also argues that Yavatkar inherently communicates statistics collected in the gateway to control center: "... statistics from the monitoring process is inherently gathered data of similarities or differences used for analysis purposes to determine the attacks and kind of traffic on the gateway." Appellant contends that no reasonable reading of Yavatkar can construe the reference as inherently collecting statistics to analyze network traffic to determine whether a gateway is under attack.

Claims 29 and 30

For the purposes of this appeal only, claims 29 and 30 stand or fall together. Claim 29 is representative of this group of claims.

Claim 29 is directed to a computer program product ... for protecting a victim site during a denial of service attack. Claim 29 includes instructions ... to monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic, communicate statistics collected in the computer device to a control center and filter out packets that the device or control center deems to be part of an attack.

---

[14] Yavatkar Col. 13, line 58 to Col. 14, line 2

Yavatkar neither describes nor suggests these features of claim 29 for analogous reasons as those given in the Appellant's arguments for claim 1. Yavatkar fails to describe or suggest instructions to communicate statistics collected in the computer device to a control center. The examiner contends that Yavatkar disclose this feature. Appellant disagrees. Rather Yavatkar discloses: "A sniffer is a device which may record network statistics at a node."[15] Similarly, Yavatkar discloses: "Worksheets 234-38 may perform tasks such as monitoring port statistics, CPU utilization, or reachability to other nodes."[16]

Neither of these teachings describes or suggests the claimed feature of: "a communication process that communicates statistics collected in the gateway by the monitoring process to a control center."

The examiner also argues that: "statistics from the monitoring process is (sic) inherently gathered data of similarities or differences used for analysis purposes to determine the attacks and kind of traffic on the gateway."[17] Applicant disagrees for the reasons discussed for claim 1. While it is arguable whether the disclosed sniffer "records network statistics at a node" meets the claimed feature of "...statistics collected in the gateway from the monitoring process... ," it is quite clear that Yavatkar does not describe: "instructions to communicate statistics collected in the computer device to a control center."

Yavatkar does not disclose any feature of the control center with the Worksheet teachings discussed above. Moreover, because Yavatkar discloses a "sniffer" as an element of the prior art, which he strongly criticizes, and discloses "Worksheets" as part of the state of the disclosed agents 110, it cannot follow that the examiner has made out a case of prima facie anticipation, since there is no disclosure in Yavatkar that uses the combined functionality of the sniffer and the worksheets. Therefore, assuming *arguendo* that somehow these two passages did teach the claimed feature, the examiner still has not made out a prima facie anticipation case, since these features being disclosed as disconnected and incompatible and indeed one being criticized by Yavatkar could not meet the test to establish anticipation, as set forth by the Federal Circuit: "Anticipation requires the presence in a single prior art disclosure of all elements of a claimed

[15] Yavatkar at Col 2, lines 4-5
[16] Yavatkar at Col. 10, lines 15-16
[17] Final Acton page 3.

invention arranged as in the claim." *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983).

Yavatkar also discloses agents, "mobile software modules" to collect data on the state of a network during a network attack. However, Yavatkar also discloses that an agent manages devices via services provided on a proxy device to monitor or control managed devices.[18] Yavatkar neither describes nor suggests instructions to communicate statistics collected in the computing device to a control center. Yavatkar's disclosed agents do not communicate or collect statistics and in particular do not communicate the statistics to a control center.

Claim 29 also requires instructions to filter. This feature also distinguishes for analogous reasons as those given in Appellant's argument for claim 1.

Appellant contends therefore that Yavatkar fails as an anticipating reference because Yavatkar fails to describe the computer program product, as claimed. The examiner's anticipation rejection is a concoction of unrelated elements from Yavatkar that existed in three separate unrelated mechanisms. However, this does not constitute an anticipatory reference since although arguable these mechanisms may have some individual relevance to the claimed features, they do not when taken together describe the claimed computer program product, since there is no device or structure or computer program product in Yavatkar that possesses all of the features of the claimed computer program product. Thus, assuming that the examiner is correct that elements from claim 1 are found in the reference, it is patently clear that those elements are not arranged in the reference in a manner as they are arranged in the claim.

The examiner also argues that Yavatkar inherently communicates statistics collected in the gateway to control center: "... statistics from the monitoring process is inherently gathered data of similarities or differences used for analysis purposes to determine the attacks and kind of traffic on the gateway.] Appellant contends that no reasonable reading of Yavatkar can construe the reference as inherently collecting statistics to analyze network traffic to determine whether a gateway is under attack.

Claims 2 and 17

[18] See Yavatkar col. 11, lines 46-55.

For the purposes of this appeal only, claims 2 and 17 stand or fall together. Claim 2 is representative of this group of claims.

Claim 2 further limits claim 1, and recites that: "the communication process couples to a dedicated link to communicate with the control center over a hardened network." This feature is not described by Yavatkar. The examiner contends that: "As per claim 2: See col.2, lines 57-59, discussing the communication process couples to a dedicated link to communicate with the control center over a hardened network." [19]

The examiner relies on the teaching in Yavatkar that the system launches an agent and has "the agent iteratively identify which of the links on the node on which the agent operates accepts a type or class of traffic, traverse the identified link to the node across the link, and repeat the process. However that is not what Appellant claims, rather Appellant claims that the there is "a dedicated link to communicate with the control center over a hardened network." Neither the agent nor the nodes are dedicated links and moreover it appears that the agent has an indeterminate destination, in contrast to the control center. There is no mention in Yavatkar that the network that the communication process uses to communicate with the control center is a dedicated, hardened network. Rather it appears to be the same network that is monitored by the agent.

Accordingly, since Yavatkar fails to describe all of the features of claim 2 arranged as in the claim, Yavatkar cannot anticipate claim 2.

Claims 5, 20 and 31

For the purposes of this appeal only, claims 5, 20 and 31 stand or fall together. Claim 5 is representative of this group of claims.

Claim 5 further limits claim 1 requiring that the gateway is adaptable to dynamically install the filters on nearby routers. The examiner argues that: "As per claim 5: See col. 14, lines 26-28 and col. 15, lines 38-39; discussing the gateway is adaptable to dynamically install filters on nearby routers."[20]

---

[19] Final Action page 4
[20] Id.

Yavatkar discloses: "A watchdog agent may perform attack monitoring using filters [8] software modules designed to detect a certain type or pattern of traffic. Filters may be dynamically added to a watchdog agent or to a system on which a watchdog agent operates according to a type of attack which may occur."[21] Appellant contends that Yavatkar's discussion that filtering can be added to the watchdog agent does not meet the claimed element that the gateway is adaptable to dynamically install filters on nearby routers. Yavatkar does not disclose that the gateway installs filters on routers. Rather, Yavatkar teaches away from this feature by:

> **In a network having multiple gateways to other networks, if the particular gateway allowing attack traffic onto the network can be identified, the attack can be halted. Either the gateway can be shut down or the appropriate filter can be installed on the gateway. However, using current methods to identify the gateway which is, in effect, the source of attack traffic to the network can be difficult and time consuming. A network administrator using a sniffer may determine which physical link (of multiple links) on a device receiving attack traffic is the source of such traffic. Certain modules resident on nodes may perform similar functions under the direction of a central console. With such information a network administrator may move from node to node, tracing the path of the hostile messages from the victim to the source, or to the gateway allowing such traffic to enter the network. Such a method of determining the source of messages is slow.** [22]

Yavatkar does mention filters, but does not describe that the filters are installed by the gateway on nearby routers.

Claims 6, 8, 9, 21, 23, 24, 32, 34 and 35

For the purposes of this appeal only, claims 6, 8, 9, 21, 23, 24, 32, 34 and 35 stand or fall together. Claim 6 is representative of this group of claims.

Claim 6 further limits claim 1 by reciting that: "the monitoring process detects IP traffic and determines levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets." The examiner relies on col. 13, lines 4-29 and col. 15, lines 30-33; of Yavatkar for this feature. Claim 8 recites that the monitoring process detects Internet Protocol (IP) traffic and determines levels of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets to unused ports, whereas claim 9 recites that the monitoring process detects IP traffic and determines levels of TCP segments advertising unusually small

[21] Yavatkar col. 15, lines 36-38
[22] Id. at col. 13, line 54 to col. 14, line 2

window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

Claim 6 will be used to argue why Yavatkar fails to disclose the features of these claims. Yavatkar discloses at col. 13, lines 4-29 the basic TCP connection protocol and how a process detects IP traffic and determines levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets." A SYN-ACK attack can take advantage of that protocol. However, neither in that passage nor elsewhere does Yavatkar describe that "the monitoring process detects IP traffic and determines levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets." Moreover, at col. 15, lines 30-33; of Yavatkar is disclosed that the watchdog agent monitors of other types of attacks by monitoring for traffic characteristics of such attacks. However, this does not describe "the monitoring process detects IP traffic and determines levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.", as required by claim 6.

Similarly, Yavatkar fails to disclose at the cited passages or elsewhere that "the monitoring process detects Internet Protocol (IP) traffic and determines levels of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets to unused ports," as in claim 8 or that "the monitoring process detects IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection," as in claim 9. Mere disclosure of he TCP connection protocol does not describe heuristics that are used to determine types of attacks.

Claims 7, 22, 33

For the purposes of this appeal only, claims 7, 22, and 33 stand or fall together. Claim 7 is representative of this group of claims.

Claim 7 further limits the gateway of claim 1 by reciting that the monitoring process detects Internet Protocol (IP) traffic and determines levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination

addresses. The examiner relies on Yavatkar at col. 13, lines 44-53 and col. 15, lines 19-21 for this feature.

Yavatkar at the cited passages discusses a spoofing attack, where the sender sends fake or false return addresses, such that the source of the attack cannot be identified from the received packets. Again, here Yavatkar merely discusses the mechanisms of such an attack, not any technique to thwart it. Nonetheless, claim 8 specifically recites to determine levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses. Yavatkar whether at col. 13, lines 44-53 and col. 15, lines 19-21 or elsewhere does not determine levels of these types of packets and therefore does not suggest this feature.

Claims 10, 25 and 36

For the purposes of this appeal only, claims 10, 25, and 36 stand or fall together. Claim 25 is representative of this group of claims.

Claim 25 limits claim 16 and recites that monitoring comprises detecting sustained rate higher than plausible for a human user over a persistent HTTP connection. The examiner contends that Yavatkar teaches this feature at col. 1, lines 27-31, which is reproduced below.

> **One method for allowing network nodes to communicate is the TCP/IP transport protocol. Modules on different nodes may use TCP/IP as a protocol to communicate with each other via a network. Every node connected to a network using TCP/IP has an internet protocol ("IP") address, which consists of four numbers, each separated a period. This IP address may be used to name the node. Some nodes may have more than one IP address.**

As with claims 6-9 discussed above, here again the examiner fails to show where Yavatkar teaches the claimed feature and instead relies on Yavatkar's discussion of the TCP/IP transport protocol. However, nothing in this passage or in the remainder of Yavatkar discloses to detect rates of reloads higher than possible for a human.[23]

Claim 11

[23] In claim 10 the word "reloads" was inadvertently omitted. Therefore, Appellant argues claim 25 but, will amend claim 10 after the Board's decision.

Claim 11, which recites that the "monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail," is neither described nor suggested by Yavatkar. The examiner relies on col.2, lines 53-55 for this feature. In that passage, Yavatkar discusses:

> **A method and system are disclosed for analyzing traffic on a network by monitoring network traffic and, when a particular network condition (for example, a network attack) is detected, gathering information about the traffic on the network by launching an agent and having the agent iteratively identify which of the links on the node on which the agent operates accepts a type or class of traffic, traverse the identified link to the node across the link, and repeat the process.**

Claim 11, although broadly worded, is not met by this passage or any other teaching in Yavatkar. Claim 11 calls for "monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail." Nowhere does Yavatkar teach to maintain statistical information or a summary of the information over different periods of time and different levels of detail. Indeed, to the extent that this discussion in Yavatkar is at all relevant to the claim, Yavatkar appears to only gather information about the traffic "when a particular network condition is detected." Yavatkar does not monitor over different periods of time and different levels of detail nor does Yavatkar teach to maintain statistical summary information over those periods and levels of detail.

Claims 12, 26 and 37

For the purposes of this appeal only, claims 12, 26 and 37 stand or fall together. Claim 12 is representative of this group of claims.

Claim 12 sets forth some of the parameters for which statistical information is provided by the monitoring process. Claim 12 recites: "statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction." Yavatkar does not describe maintaining statistical information on these specific parameters, whether at col.2, lines 4-5 or col.3, lines 30-32 or elsewhere in Yavatkar.

Indeed, the examiner conflates two unrelated concepts from Yavatkar. One is the discussion of a sniffer, "A sniffer is a device which may record network statistics at a node." and

the other is a discussion concerning Yavatkar's invention, "During a network attack, the system and method of the present invention allow for details on the attack traffic (e.g., the source of the attack traffic and path of the attack traffic) to be gathered. The source of the attack traffic may be the originator of the attack traffic or, for example a gateway allowing attack traffic to enter a network and which is, in effect, the source of attack traffic to the network. Such information then may be used to halt the attack or insulate the network from the attack." However, Yavatkar at Col. 3, lines 30-32 does not describe to maintain statistical information but instead teaches to trace paths of an attack using the bloodhound and watchdog agents discussed later by Yavatkar. Indeed, Yavatkar mentions that the sniffer concept is slow.[24]

Claims 13, 27 and 38

For the purposes of this appeal only, claims 13, 27 and 38 stand or fall together. Claim 13 is representative of this group of claims.

Claim 13 recites that the "monitoring process has configurable thresholds and issues a warning when one of the measured parameters exceeds the corresponding threshold." The examiner relies on col. 14, lines 54-58 and col. 15, lines 26-27 for this feature. However, at col. 14, lines 54-58 Yavatkar discusses that the watchdog agents can enter an alert mode where it can create bloodhound agents and col. 15, lines 26-27, where Yavatkar discusses where the watchdog agent can interface with software controlling the three way handshake of the TCP/IP connection protocol. However, none of these discussions describes "configurable thresholds" or that the

[24] Systems exist for collecting information about network traffic. For example, to determine the node which is the source of attack traffic (or the gateway allowing such traffic into a network, which in such a case may be considered a source) and the path or paths taken by such traffic, a human operator may access each link at a node receiving such traffic and analyze the incoming traffic using a sniffer. A sniffer is a device which may record network statistics at a node. The operator may identify which of the physical links attached to the node is receiving a certain type or amount of traffic and then move to the node on the other end of the identified link. The path or paths of traffic from the source of the traffic may be found by traversing the network from node to node, using the sniffer at each node in a path, until the source is reached. Such a diagnosis is slow and inaccurate. A similar analysis may be performed from a central console which may query remote nodes for information about the source of incoming traffic. Such a diagnosis is also slow and inaccurate, as it requires commands to nodes and responses from nodes to be transmitted across the network. The speed at which attacks occur and the speed at which such problems must be fixed makes such detection methods ineffective. A path taken by traffic may be described as the equipment traversed by traffic as the traffic crosses a network or networks (e.g., a series of nodes and links, or a series of sub-networks). Yavatkar Col.1, line 65 to col. 2, line 23.

gateway issues a warning when one of the measured parameters exceeds the corresponding threshold.

Claim 39

Claim 39 distinguishes Yavatkar does not describe "... instructions to cause the processor to receive communications from a control center to deliver data pertaining to the types of traffic passing through the gateway."[25]

Conclusion

Appellant submits, therefore, that Claims 1-39 are not anticipated by Yavatkar are allowable over the cited art. Therefore, the Examiner erred in rejecting Appellant's claims and should be reversed.

Respectfully submitted,

Date: 2/13/07

Dennis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21515162.doc

[25] In claim 39 there is not antecedent basis for "processor" and "gateway," but functionally those are equivalent to the "computing device" recited in base claim 29. Appellant will amend this claim after the Board's decision.

Appendix of Claims

1. A gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device comprises:

a computing device comprising;

a monitoring process that monitors network traffic through the gateway;

a communication process that communicates statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center; and

a filtering process to insert filters on network devices to filter out packets that the gateway deems to be part of an attack.

2. The gateway of claim 1 wherein the communication process couples to a dedicated link to communicate with the control center over a hardened network.

3. The gateway of claim 1 wherein the monitoring process in the gateway samples network packet flow in the network.

4. The gateway of claim 1 wherein the gateway is adaptable to be physically deployed in line in the network.

5. The gateway of claim 1 wherein, the gateway is adaptable to dynamically install the filters on nearby routers.

6. The gateway of claim 1 wherein the monitoring process detects IP traffic and determines levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

7. The gateway of claim 1 wherein the monitoring process detects Internet Protocol (IP) traffic and determines levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

8. The gateway of claim 1 wherein monitoring process detects Internet Protocol (IP) traffic and determines levels of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets to unused ports.

9. The gateway of claim 1 wherein monitoring process detects IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

10. The gateway of claim 1 wherein monitoring process detects sustained rate higher than plausible for a human user over a persistent HTTP connection.

11. The gateway of claim 1 wherein monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail.

12. The gateway of claim 11 wherein monitoring process maintains statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

13. The gateway of claim 12 wherein monitoring process has configurable thresholds and issues a warning when one of the measured parameters exceeds the corresponding threshold.

14. The gateway of claim 13 wherein monitoring process logs packets.

15. The gateway of claim 14 wherein monitoring process logs specific packets identified as part of an attack to enable an administrator to identify important properties of the attack.

16. A method of protecting a victim site during a denial of service attack, comprises:

disposing a gateway device between the victim site and a network;

monitoring network traffic through the gateway and measuring heuristics of the network traffic to provide statistics network traffic;

communicating the statistics collected in the gateway to a control center; and

filtering out packets that the gateway or control center deems to be part of an attack.

17. The method of claim 16 wherein communicating occurs over a dedicated link to the control center via a hardened network.

18. The method of claim 16 wherein monitoring samples network packet flow in the network.

19. The method of claim 16 wherein the gateway is physically deployed in line in the network.

20. The method of claim 16 wherein filtering further comprises:

dynamically installing filters on nearby routers via an out of band connection.

21. The method of claim 16 wherein monitoring further comprises:

detecting IP traffic and determining levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

22. The method of claim 16 wherein monitoring further comprises:

detecting Internet Protocol (IP) traffic and determining levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

23. The method of claim 16 wherein monitoring further comprises:

detecting Internet Protocol (IP) traffic and determining levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

24. The method of claim 16 wherein monitoring further comprises:

detecting IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

25. The method of claim 16 wherein monitoring further comprises:

detecting a sustained rate of reload requests that is higher than plausible for a human user over a persistent HTTP connection.

26. The method of claim 16 wherein monitoring further comprises:

logging statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

27. The method of claim 16 wherein monitoring further comprises:

issuing a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

28. The method of claim 16 wherein monitoring further comprises:

logging specific packets identified as part of an attack to enable an administrator to identify important properties of the attack.

29. A computer program product residing on a computer readable medium for protecting a victim site during a denial of service attack, comprises instructions for causing a computer device coupled at an entry to the site to:

monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic;

communicate statistics collected in the computer device to a control center; and

filter out packets that the device or control center deems to be part of an attack.

30. The computer program product of claim 29 wherein instructions to monitor further comprise instructions to:

sample network traffic flow.

31. The computer program product of claim 29 wherein instructions to filter further comprise instructions to:

dynamically install filters on nearby routers via an out of band connection.

32. The computer program product of claim 29 wherein instructions to monitor further comprise instructions to:

detect IP traffic; and

determine levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

33. The computer program product of claim 29 wherein instructions to monitor further comprise instructions to:

detect Internet Protocol (IP) traffic; and

determine levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

34. The computer program product of claim 29 wherein instructions to monitor further comprise instructions to:

detect Internet Protocol (IP) traffic; and

determine levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

35. The computer program product of claim 29 wherein instructions to monitor further comprises instructions to:

detect IP traffic; and

determine levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

36. The computer program product of claim 29 wherein instructions to monitor further comprises instructions to:

detect a sustained rate of reload requests that is higher than plausible for a human user over a persistent HTTP connection.

37. The computer program product of claim 29 wherein instructions to monitor further comprises instructions to:

log statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

38. The computer program product of claim 29 wherein instructions to monitor further comprises instructions to:

issue a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

39. The computer program of claim 29 further comprising instructions to cause the processor to receive communications from a control center to deliver data pertaining to the types

of traffic passing through the gateway.

Evidence Appendix

None

Related Proceedings Appendix

None